

OUCH!

本期导读

- 概览
- 密码
- 两步验证

两步验证

概览

证明你是谁的过程（称之为“验证”）是保护信息的关键。强验证试图确保只有你才能访问你的邮件、照片、银行账户等信息。有三种方式确认你的身份：你所知道的——如密码，你所拥有的——如驾照，你所是——如指纹。这三种方式均有各自的优缺点。最常见的方式就是密码了，即通过你所知道的确认你的身

份。本期，我们将教你如何使用两步验证来保护自己，这种方式比单纯使用密码要安全很多，而其自身使用起来又相当简单。为了更好地理解两步验证，我们先得从密码开始讲起。

客座编辑

Keith Palmgren在信息安全领域有超过30年的从业经历。他是SANS认证讲师以及五日信息安全导论课程“SANS SEC301”的作者。授课之外，他专注于顾问和书面工程。你可以在Twitter上关注他（@kpalmgren）。

密码

密码根据你所知道的来证明你的身份。其风险在于密码一旦泄露就不存在任何保护了，猜到或者获得你密码的人能装作是你并访问其保护下的你的任何信息。这也就是为什么别人教你使用难以猜解的强密码、针对每个账号使用不同的密码、绝不向任何人透露自己的密码，从而保护你的密码。这条建议仍然有效，然而密码的效用却大不如前了，它们在当下不再有效。最新的科技让网络攻击者能轻而易举地破解密码。我们需要一个易于使用同时更加安全的强验证手段。幸运的是，这一选项在很多地方都可用，它就叫做“两步验证”。

两步验证

两步验证（有时叫做“双因素验证”或者“2FA”）是一种比密码更加安全的解决方案。它要求用户通过两种而非一种方式证明自己的身份。银行卡就是一个例子，当你从ATM取钱时，你实际上就在使用一种形式的两步验

两步验证

证。要取钱你需要两个东西：银行卡（你所拥有的）和密码（你所知道的）。如果你银行卡丢了，钱仍是安全的。捡到银行卡的人无法取走你的账款，因为他们不知道你的密码；（除非你把密码写在了卡上，而这是个坏主意。）同样，如果他们知道你的密码却没有你的卡，他们还是不能取钱。攻击者必须同时满足两项条件才能攻破你的银行账户。这也就是为什么两步验证安全更多，你有两层安全防护。

使用两步验证

你需要针对你的每个账号单独设置两步验证。幸运的是，如今很多在线服务都提供两步验证的选项。Google就是两步验证的领军者之一。由于Google为全世界数百万人提供诸多免费的在线服

务，Google账号成为了网络攻击者的首选目标。因此，Google需要提供更强有力的验证方式，事实上它也是首批针对其大多数在线服务开通两步验证方式的组织之一。如果你理解Google两步验证的工作方式，你就能理解Twitter、Facebook、Apple、Instagram和许多银行及其它网站的两步验证的原理。

首先，启用Google账号上的两步验证，并注册手机号。完成后，两步验证就生效了。你如往常一样用用户名和密码登录账号，这就是双因素中的第一个因素——你所知道的。Google之后会向你的手机发送一条短信，其中包含一段由6个数字组成的独一无二的安全码。正如密码一样，你需要在网站上输入这个安全码。这就是双因素中的第二个因素。因此，要成功登录你的账号，你需要知道你的密码，并且还要用你的手机来接收安全码。即便攻击者知道你的密码，他们还是不能访问你的Google账号，除非他们还有你的手机。为确保你的账号真正安全，Google会在你每次登录时向你发送一条新的唯一的安全码。



尽可能使用两步验证，它是你能采取的最强的保护个人信息的方式之一。

两步验证

针对Google和许多其它网站的两步验证，还有另外一个选项。除了通过短信来接收安全码外，你还可以在智能手机上安装验证APP。APP会在你每次要登录时为你生成独一无二的安全码。这样做的优点就是你不用连接手机运营商服务来接收你的安全码，你的手机会为你生成；此外，由于安全码是本地生成而非接收到的，它无法被截获。

记住，两步验证默认并未启用，你得自己启用它。尽管两步验证可能最初会看似多了不少麻烦，我们强烈建议，只要有可能就使用它，尤其是针对邮箱帐号、网上银行、网络存储等关键服务。相比密码，两步验证在保护你的信息的路上要走得远得多。

了解更多

订阅OUCH! 安全意识月刊，访问OUCH! 过往存档，了解更多关于SANS安全意识解决方案的信息，请访问：<http://www.securingthehuman.org>.

相关资源

密文:	http://www.securingthehuman.org/ouch/2015#april2015
支持两步验证的网站:	https://twofactorauth.org
Stop Think Connect:	http://stopthinkconnect.org/2stepsahead
Google两步验证:	http://www.google.com/landing/2step/
SANS每日安全贴士:	http://www.sans.org/tip_of_the_day.php

OUCH! 由SANS Securing The Human出版，根据 "[知识共享许可协议4.0 \(署名-非商业使用-禁止演绎\)](#)" 发行。你可以在不对其进行修改的前提下，自由传播这份新闻简报或在你的安全意识课程中使用它。了解翻译或更多信息，请联系：ouch@securingthehuman.org。

编委: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
翻译: 成自豪



securingthehuman.org/blog



[/securethehuman](https://securethehuman)



[@securethehuman](https://twitter.com/securethehuman)



securingthehuman.org/gplus